#14

1 of 3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Attorney Docket No. **RP9-99-048**

In re Application of: §
§
CROMER ET AL. §
§ Examiner: **LEE, C.**
Serial No. **09/281,852** §
§ Art Unit: **2131**
Filed: **31 MARCH 1999** §
§
For: **DATA PROCESSING SYSTEM** §
AND METHOD FOR MAINTAINING §
SECURE DATA BLOCKS §

APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is submitted in triplicate in support of the Appeal in the above-identified application.

CERTIFICATE OF MAILING
37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as First-Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date below.

11/20/03
Date

Catherine D. Nelson
Signature

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, the real party of interest.

RELATED APPEALS AND INTERFERENCES

No related appeal is presently pending.

STATUS OF THE CLAIMS

Claims 1-7 and 10-16 stand finally rejected by the Examiner as noted in the Final Office Action dated August 13, 2003 and the Advisory Action dated October 22, 2003.

STATUS OF AMENDMENTS

No amendment was submitted subsequent to the Office Action dated 8 January, 2003.

SUMMARY OF THE INVENTION

A website may send a block of data, commonly known as a *cookie*, to a user's computer system for the purpose of facilitating subsequent access to the website. The cookie may include public information pertaining to the website as well as private information associated with the user. With respect to a user's private information, a cookie may include, *inter alia*, a username along with a corresponding password, the user's credit card information, the user's address, and the user's online usage preferences. Because it is paramount to maintain the data security of cookies when private information are involved, it is most preferable to store cookies in a secure storage area of a user's computer system.

During each website access, a user's computer may receive cookies that need to be stored in a secure storage area of the user's computer system. Thus, over time, it is most likely that the number of cookies will eventually exceed the size of the secure storage area within the user's computer system. But if the "overflow" cookies are stored in a non-secured storage area of the user's computer system, such as a hard disk drive, it is foreseeable that an unauthorized user can copy a user's cookies from the user's computer system to another computer system for the purpose of extracting valuable information stored within the cookies. Therefore, it is desirable to provide a method for storing cookies in a non-secured mass storage device within a user's computer system while without sacrificing the data security of the cookies.

In accordance with a preferred embodiment of the present invention, an encryption key pair, which includes a private key and a public key, is stored in a protected storage device within a data processing system, as shown in block **304** of Figure **3**. In response to the receipt of a cookie generated by an application from a remote server, the cookie is encrypted with the public key of the encryption key pair, as depicted in block **308** of Figure **3**. The encrypted cookie can now be stored in a non-protected storage device, such as a hard disk drive, within the data processing system, as shown in block **310** of Figure **3**. In response to an access request for the encrypted cookie by a browser program executing within the data processing system, a copy of the encrypted cookie is sent to the protected storage device, as depicted in block **408** of Figure **4**, and the encrypted cookie is decrypted using the private key within the protected storage device, as shown in block **410** of Figure **4**. Finally, the decrypted cookie is sent to the browser program requesting the cookie, as shown in block **412** of Figure **4**.

ISSUE

Is the Examiner's rejection of Claims 1-7 and 10-16 under 35 U.S.C. § 103(a) as being unpatentable over *Nielsen* (US 6,006,333) in view of *Pond et al.* (US 4,864,616) and *Schneier*, Applied Cryptography, 2nd edition, John Wiley & Sons, Inc., 1996 well-founded?

GROUPING OF THE CLAIMS

For purposes of this Appeal, Claims 1-7 and 10-16 stand or fall together as a single group.

ARGUMENT

The Examiner's rejections of Claims 1-7 and 10-16 are not well-founded and should be reversed.

I. The claimed cookie comes from "an application from a remote server" and not from a user

Claim 1 (and similarly Claim 10) recites a step of "in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key." Thus, according to the claimed invention, the cookie is originated from an application within a remote server. On page 2 of the Final Office Action, the Examiner analogized the user IDs and passwords of *Nielsen* as the claimed cookie. However, the user IDs and passwords of *Nielsen* are different from the claimed cookie because the user IDs and passwords of *Nielsen* are manually entered by a user either ahead of time (col. 5, lines 44-47) or in response to a request in real time (col. 6, lines 12-14). In contrast, the claimed cookie comes from "an application from a remote server," and not from a user.

Also, the encryption of the claimed cookie with a public key is performed "in response to the receipt of ... [the claimed] cookie. In other words, the cookie encryption is performed automatically once the claimed cookie is received from a remote server without any user intervention.

II. The conflicting teachings of *Nielsen* and *Pond* cannot be reconciled by a person of ordinary skill in the art

Claim 1 recites steps of "storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system" and "encrypting said cookie with said public key." Thus, according to the claimed invention, the cookie is encrypted by a public key previously stored in a protected storage device within a data processing system. In contrast, according to *Nielsen*, the user IDs and passwords are encrypted by a master password entered by a user after being prompted (col. 4, line 31). Even though *Nielsen* also teaches that the master password can be stored in a storage device, but according to *Nielsen*, the master password is stored in a system memory (col. 4, lines 31-32). Since the system memory is a non-protected device, *Nielsen*'s teachings are different from the teachings of the claimed invention.

Moreover, since *Nielsen* has already offered a better solution for enhancing the security of the master password, and that is "never store the master password" (col. 4, lines 36-37). In light of such teachings by *Nielsen*, it would not have been obvious to one skilled in the art to store the master password in a protected storage device similar to what is disclosed in *Pond*, as suggested by the Examiner on page 3 of the Final Office Action. In order to combine the teachings of *Nielsen* and *Pond* for rendering the claimed invention obvious, the Examiner is required to overcome the above-mentioned conflict between the teachings of *Nielsen* and *Pond*. This is because according to MPEP § 2143.01, when there is a conflict between the teachings of two or more prior art references, "the Examiner must weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another" (emphasis added).

On page 2 of the Advisory Action, the Examiner asserts that "Nielsen discloses the choice to store the master password or not to store the master password so that the step 304 can be skipped (see column 4 lines 35-37)." Appellants disagree with the Examiner's interpretation of skipping step **304** as the reason for choosing between storing and not storing a master password according to *Nielsen*. This is because *Nielsen* continues to explain if a user chooses to never store a master password, "the user is prompted for the master password whenever it is needed ... [and this] provides enhanced security in that unauthorized persons will not be able to access remote sites when client computer system **10** is left unattended with its browser software running." Thus, it is clear that skipping step **304** is not the reason for choosing between storing and not storing a master password, as suggested by the Examiner. As such, the Examiner ultimately did not demonstrate how the conflicting teachings of *Nielsen* and *Pond* could be reconciled by a person of ordinary skill in the art. Therefore, the combination of *Nielsen* and *Pond* for the § 103 rejection is improper.

III. The cited references do not teach or suggest the claimed encrypting and decrypting steps

Even though both *Pond* and *Schneier* are related to cryptography, neither *Pond* nor *Schneier* teaches or suggests the claimed steps of "encrypting said cookie with said public key" and "decrypting said encrypted cookie with said private key." Col. 6, lines 35-63 of *Pond* teaches data entered into a protected file is first encrypted under a Mandatory Key Stream **20** and then under each of the other key streams designated by a Key Mix **36**. *Pond* further explains that based on Key Mix **36** designated during the creation of the protected file, the file can only be decrypted under one of the four conditions listed in col. 6, lines 45-54. There is no teaching or suggestion in *Pond* as to the claimed "encrypting said cookie with said public key" and "decrypting said encrypted cookie with said private key." Because the cited references, whether considered separately or in combination, do not teach or suggest the claimed invention, the § 103 rejection is improper.

CONCLUSION

For the reasons stated above, Appellants believe that the claimed invention clearly is patentably distinct over the cited references and that the rejections under 35 U.S.C. § 103 are not well-founded. Hence, Appellants respectfully urge the Board to reverse the Examiner's rejection.

Please charge the IBM Deposit Account **50-0563** in the amount of $440.00 for submission of a Brief in support of Appeal and one month extension of time. No additional fee or extension of time is believed to be required; however, in the event an additional fee or extension of time is required, please charge that fee or extension of time requested to the IBM Deposit Account **50-0563**.

Respectfully submitted,

Antony P. Ng
Registration No. 43,427
BRACEWELL & PATTERSON, LLP
111 Congress Avenue, Suite 2300
Austin, Texas 78701
512.542.2134

ATTORNEY FOR APPELLANTS

APPENDIX

1. A method for protecting the security of a cookie stored within a data processing system, said method comprising:

storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system;

in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key;

storing said encrypted cookie in a non-protected storage device within said data processing system;

in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key; and

sending said decrypted cookie to said browser program.

2. The method according to claim 1, wherein said non-protected storage device is a hard drive.

3. The method according to claim 1, further comprising providing an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine.

4. The method according to claim 3, wherein said encrypting further include encrypting said cookie utilizing said encryption device.

5. The method according to claim 4, wherein said decrypting further includes decrypting said encrypted cookie utilizing said encryption device.

6. The method according to claim 5, wherein said sending further includes transmitting said decrypted cookie from said encryption device to said browser program.

7. The method according to claim 6, further comprising transmitting said decrypted cookie from said browser program to an application executing in a remote server.

10. A data processing system capable of protecting the security of a cookie stored within said data processing system, said data processing comprising:

a protected storage device for storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system;

means for utilizing said public key to encrypt said cookie, in response to the receipt of a cookie generated by an application from a remote server;

a non-protected storage device within said data processing system for storing encrypted cookie;

means for utilizing said private key to decrypt said encrypted cookie, in response to an access request for said encrypted cookie by a browser program executing within said data processing system; and

means for sending said decrypted cookie to said browser program.

11. The data processing system according to claim 10, wherein said non-protected storage device is a hard drive.

12. The data processing system according to claim 10, further comprising an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine.

13. The data processing system according to claim 12, wherein said means for utilizing said public key to encrypt said cookie is said encryption engine.

14. The data processing system according to claim 13, wherein said means for utilizing said private key to decrypt said encrypted cookie is said encryption device.

15. The data processing system according to claim 14, wherein said sending means further includes means for transmitting said decrypted cookie from said encryption device to said browser program.

16. The data processing system according to claim 15, further comprising means for transmitting said decrypted cookie from said browser program to an application executing in a remote server.